

ANNEX 1. TECHNICAL SPECIFICATIONS FOR COMBRIDGE PRODUCTS AND SERVICES

1. General Description

CPE-A (Smart CPE Advance) - equipment with 3G backup, Cloud-based equipment management, 4x Gigabit Ethernet LAN

IACC (Combridge Internet Access) - Internet access provided by Combridge via fibre optics; 100 Mbps; public IP address

VPN (Virtual Private Network) - Connecting locations via virtual private networks (VPNs)

CCS (Corporate Communication Solution) - Corporate IP PBX communication solution; Firewall; DDoS; Content filtering; Fax2Mail/Mail2Fax; Hosting; Mail server

CCS-E - Entry Corporate Communication Solution for up to 20 users

CCS-A - Advanced Corporate Communication Solution for an unlimited number of users

VPS-E - Easy Virtual Private Server

VPS-A - Advanced Virtual Private Server

VPS-S - Star Virtual Private Server

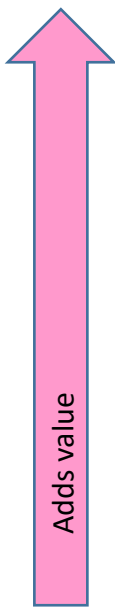
MLAN/MWLAN - Wired or wireless local area network management.

HBV/M/HE/EX - basic/medium/high end/executive voice headsets, i.e. basic (B), medium (M), high end (HE), executive (EX) IP phones.

LBA, LPL; LPR - Linkyfi basic (LBA), Plus (LPL) and Pro (LPR) WiFi marketing platform.

MWL-CMBW-ANM and MWL-CMBW-RNM - network management platform

The ordering process is simple, Cloud-based (Smart CPE) and functionalities are added according to the company's needs, as shown in Figure 1.



Services				Added benefits
Smart CPE-A	VPN	CC S-A/E	MLAN/MWLAN*	Managed LAN/WLAN
Smart CPE-A	VPN	CC S-A/E	VHHE*+VHEX*	Executive extension mode
			VHHE*	IP telephone with Gigabit port and Bluetooth
			VHM*	IP telephone with Gigabit Port
			VHB*	IP telephone
Smart CPE-A	VPN	CC S-A/E	VPS-S	Star VPS processing power
			VPS-A	Advanced VPS processing power
			VPS-E	Easy VPS processing power
Smart CPE-A	VPN	CC S-A		IP PBX; Firewall; DDoS; Content filtering; Hosting; Fax2Mail/Mail2Fax; Mail server; unlimited users
		CC S-E		IP PBX; Firewall; DDoS; Content filtering; Hosting; Fax2Mail/Mail2Fax; Mail server; up to 20 users
Smart CPE-A	VPN			Provides a virtual private network (VPN) between locations
Smart CPE-A				Advanced: 4G backup; Cloud-based equipment management; 802.11 b/g/n; 4 Gigabit Ethernet LAN ports

Figure 1.

*Ordering codes:

Managed LAN: MLAN-8P-SEL-1YR/3YR, MLAN-24P-E-SEL-1YR/3YR, MLAN-24P-A-SEL-1YR/3YR, MLAN-48P-SEL-1YR/3YR, MLAN-8P-CON-1YR/3YR, MLAN-24P-E-CON-1YR/3YR, MLAN-24P-A-CON-1YR/3YR, MLAN-48P-CON-1YR/3YR

Managed WLAN: MWL-122-CON-1YR, MWL-130-CON-1YR/3YR, MWL-230-CON-1YR/3YR, MWL-245-CON-1YR/3YR, MWL-250-CON-1YR/3YR, MWL-550-CON-1YR/3YR, MWL-1130-CON-1YR/3YR, MWL-122-SEL-1YR, MWL-130-SEL-1YR/3YR, MWL-230-SEL-1YR/3YR, MWL-245-SEL-1YR/3YR, MWL-250-SEL-1YR/3YR, MWL-550-SEL-1YR/3YR, MWL-1130-SEL-1YR/3YR

The services above are detailed in the following chapters.

2. Smart CPE Advanced (CPE-A)

Smart CPE Advanced (CPE-A):

- 3G Backup: Yes
- Unlimited traffic
- LAN: 5xGigaEth
- PoE: 2 ports
- Wlan: 802.11a/b/g/n

The Combridge smart equipment, available with both POE power and with radio options, offers small and medium-sized businesses a complete VPN solution with 3G backup and the ability to remotely configure the equipment. The solution is advantageous and stable both for wire-connected users and for wireless- or remote-connected ones. The unlimited traffic via both the main Internet connection and the 3G backup connection offers a clear perspective of the monthly operating cost.

The advantages of Smart CPE:

- Scalable in relation to configuration changes and minimal effort required to reconfigure the network if access locations are added in the client's network.
- Management of remote workstations
- The management is cloud-based, the cloud server is hosted in a Tier IV SAS 70, Type II colocation centre, with automatic backups and disaster recovery capabilities.
- It makes available the wireless SSID functionality
- Efficient bandwidth allocation
- Equipment suitable for both VPN and Internet

Characteristics:

- **Flexible and reliable connectivity**

With the Layer 3 IPsec VPN Combridge solution, the workstations easily and securely access the company's Intranet, maintaining total control over the information flow. Featuring integrated access control (AC) and the ability to display statistics, CPE-A can make forwarding decisions based on the user identity or device type, thus securing the Intranet access while providing connectivity to view and configure new workstations.

- **Enterprise Class Wi-Fi Security**

CPE-A is fitted with a spectral analysis module, to identify legitimate data flows, as well as with an wireless intrusion prevention system (WIPS), without requiring additional licensing fees. These features enable the

administrator to identify any possible WiFi interference, make development plans and make available to the branches stable and secure access, compliant with the applicable standards.

- **Secure switching to on-demand deployment**

CPE-A offers robust switching functionality, in line with the Wi-Fi infrastructure, including a unified bandwidth allocation, management and reporting policy. CPE-A can be activated by simply sending and connecting the equipment to a network with Internet access, and it will automatically find the network management system (NMS) from where it will download its configuration, the security policies associated with the company and will instantly provide services to the connected devices.

- **Extended security**

A single unified policy provides security and access control measures for a user. This allows control on the manner and time a user can connect via wire or wireless to the Intranet, ensuring security regardless of the connection mode.

An Internet connection is required to activate Smart CPE, and it can be:

- Internet access provided by Combridge (IACC)
- The client's Internet access

2.1. Internet access provided by Combridge (IACC)

The Combridge network covers most major cities in Romania.

The IP services are implemented on the MPLS network of the Deutsche Telekom/Magyar Telekom group.

IACC Features:

- **FTTB (Fibre to the Building) solution**
- **Public IP**
- **100 Mbps guaranteed transfer speed (upload/download)**
- **Symmetrical use**
- Guaranteed average latency of 0.03 ms/km
- Average packet loss below 0.5%
- Dedicated connection with 99.5% guaranteed SLA
- Unlimited traffic
- Online statistics
- 24/7/365 technical support
- Quarterly performance analyses

Technical terms and conditions for the provision of Internet services by Combridge

2.1.1. Definition of terms

2.1.1.1. Internet - the global network of public and private communication equipment interconnected and using the TCP/IP suite of protocols.

2.1.1.2. COMBRIDGE network - the COMBRIDGE communication equipment network (owned by COMBRIDGE or rented by COMBRIDGE) connected to the Internet through one or more points and using the TCP/IP suite of protocols.

2.1.1.3. COMBRIDGE system - the communication system of COMBRIDGE, part of the COMBRIDGE network, to which the Beneficiary connects; the system consists of: optical fibre, optical nodes, coaxial cable, RF amplifiers, distribution boxes, radio cells.

2.1.1.4. Traffic - any transfer of information performed by the Beneficiary outside the COMBRIDGE network and/or to the Beneficiary from outside the COMBRIDGE network, not including the transfer performed by the Beneficiary in the provider's network and/or to the Beneficiary in the provider's network.

2.1.1.5. Layer 1, Layer 2 and Layer 3 - layers 1, 2 and 3 of the OSI ISO (Open Systems Interconnection model of the International Organisation for Standardisation) reference model.

2.1.1.6. COMBRIDGE network access equipment, hereinafter referred to as the "Access Equipment", is the equipment connected directly (Layer 1 or Layer 2) to the COMBRIDGE network.

This includes (without limitation): cable modem, radio modem, leased line modem, fibre optic media converter, switch owned by COMBRIDGE.

2.1.1.7. Layer 2 interface connected with the COMBRIDGE network, hereinafter referred to as "the interface directly connected to the COMBRIDGE network", is any network interface (e.g. network card) of the Beneficiary which is Layer2 connected to any "Access Equipment". This includes (without limitation) equipment directly connected in the "Access Equipment" or connected through one or more Layer1 or Layer2 equipment (hubs, bridges, or switches). This does not include the Beneficiary's equipment which is separated from the "Access Equipment" by a Layer3 equipment (e.g. router).

2.1.2. Commissioning of the service

2.1.2.1. For the Internet Access and data communications service, COMBRIDGE undertakes to install and commission the service according to the installation data specified in the service commissioning protocol.

During the performance of the contract, the Beneficiary may request the relocation of a location where the services are provided, an operation the costs of which will be invoiced according to the COMBRIDGE offer in force at the date of the request.

2.1.2.2. The Beneficiary has the following obligations:

- a) To designate and prepare the locations for the installation of the equipment;
- b) To ensure the access of the COMBRIDGE personnel in charge with the installation and commissioning of the service to the internal and external buildings where the COMBRIDGE system must be placed;
- c) To facilitate the obtaining of approvals (if applicable) for the installation of the COMBRIDGE system.

2.1.2.3. The works for the commissioning of the Internet Access and data communications service are deemed as completed and the service is deemed as operational on the date of signing the commissioning protocol, or on the date provided in any other direct or indirect means of proof. If the Beneficiary refuses to sign the commissioning protocol or if the commissioning protocol cannot be drawn up for any other reason, the service will be deemed to have been commissioned unless the Beneficiary sends a written notification to the contrary, within 24 hours from the date of commissioning of the access equipment, according to the internal COMBRIDGE records.

2.1.2.4. For the installation by COMBRIDGE, in the locations covered by the contract, of circuits that allow electronic communications (circuits that may include, by way of example, cables, accessories, connectors or other materials, and the activation of the Internet Access and data communications service, the Beneficiary owes an installation fee, accounting for the value of all materials used, as recorded in the service commissioning protocol.

The installation, connection, and configuration of the Beneficiary's local area network (LAN) equipment to the end equipment are to be performed exclusively by the Beneficiary.

2.1.2.5. COMBRIDGE can provide, upon the request by the Beneficiary, the installation, connection and configuration of the Beneficiary's local network equipment to the end equipment. COMBRIDGE will invoice to the Beneficiary the equivalent value of the operations performed.

2.1.2.6. These specific clauses for Internet Access and data communications are duly supplemented by the clauses contained in Annex no. 1, which are applicable by analogy.

2.1.3. Rights and obligations of the parties

2.1.3.1. By using sufficient capacity, COMBRIDGE will continuously operate the COMBRIDGE network and the COMBRIDGE network connections to the Internet. COMBRIDGE warrants that the traffic needs of the Beneficiary will be met 365 days a year, 24 hours a day, except when the international connection is not operational due for reasons beyond COMBRIDGE's control (e.g. the failure of the telecommunications satellite, of national and international terrestrial networks providing access to the Internet network), the failure of the electricity network (the electricity provider) or any other third party COMBRIDGE concluded a contract with.

2.1.3.2. COMBRIDGE will not restrict the Beneficiary's access to any destination on the Internet. COMBRIDGE or other providers may sometimes restrict access to certain destinations for reasons of network security or protection and the Beneficiary understands that COMBRIDGE is not responsible for such actions.

2.1.3.3. COMBRIDGE will also provide backup for the international infrastructure to the extent of the possibilities of collaboration with other local Internet Service Providers, or through its own means.

2.1.3.4. COMBRIDGE is responsible for the repair of any COMBRIDGE equipment in operation, within the COMBRIDGE network, if the failure of the equipment has not occurred due to the fault of the Beneficiary or of another person for whom COMBRIDGE is not responsible. If this is not possible, the equipment will be replaced.

2.1.3.5. The Beneficiary understands that the sole beneficiary of the licenses and rights related to the operation of the COMBRIDGE System is COMBRIDGE and that such licenses and rights are exclusively related to the COMBRIDGE System.

2.1.3.6. The COMBRIDGE system can be relocated only by COMBRIDGE.

2.1.3.7. The Beneficiary will not seize, disassemble or decommission any equipment owned by COMBRIDGE.

2.1.3.8. If the Beneficiary wishes to provide to third parties services covered by this contract, the Beneficiary undertakes to request the written consent of COMBRIDGE before commencing the collaboration with such third parties. This provision is valid regardless of whether the services to third parties are provided via the COMBRIDGE system or via another infrastructure.

2.1.3.9. COMBRIDGE undertakes to continuously supervise the service and to regularly supervise (checks, inspections, etc.) the system. In order to facilitate the fulfilment of this obligation and based on a prior notification by COMBRIDGE, the Beneficiary will allow access of the COMBRIDGE technicians to the data transmission system, for them to be able to carry out the technical supervision and to verify the proper operation of the equipment.

2.1.3.10. The Beneficiary undertakes not to use outside the system, not to copy and not to disclose to third parties any software application and/or know-how implemented by COMBRIDGE. The Beneficiary will be liable for any damages and claims arising from the violation of this provision.

2.1.3.11. The Beneficiary undertakes to comply with the provisions of Section 2.1.5.

If the Beneficiary violates the provisions of Section 2.1.5, COMBRIDGE may suspend, for an indefinite period, without prior notice, in whole or in part, the services provided to the Beneficiary, until the parties clarify the situation that led to such suspension and only after the submission of explanations in writing by the Beneficiary. Furthermore, COMBRIDGE will temporarily or permanently interrupt the transmission through the COMBRIDGE network or the storage of the information sent or received by the Beneficiary, in particular by removing information or blocking access to it, the access to a communication network or the provision of any other service of the information company, if such measures were ordered by a public authority (according to the legal provisions).

2.1.3.12. COMBRIDGE will observe the confidentiality of the Beneficiary's data transferred through the COMBRIDGE network. COMBRIDGE reserves the right to delete any information introduced by the Beneficiary in the COMBRIDGE network which could affect its proper operation or could lead to the interruption of the operation of the COMBRIDGE network.

2.1.4. Security The Beneficiary undertakes to ensure the security of the network, computers and other components of its network. COMBRIDGE disclaims any responsibility for security problems in the Beneficiary's network, as the obligation to ensure the security of the network lies exclusively with the Beneficiary

2.1.4.1. The Beneficiary represents to agree to receive from COMBRIDGE information related to the service provided by COMBRIDGE, other services provided by COMBRIDGE, as well as any other commercial communications by email, post, fax or any other means deemed appropriate by the Provider.

2.1.4.2. The Beneficiary undertakes to request in writing from COMBRIDGE any information related to the contracted service only through its authorized representatives. If such requests are made by other persons, who are not authorized, COMBRIDGE will receive these requests, send them to the authorized representatives of the Beneficiary and send the answer upon request only after one of the authorized persons confirms in writing the validity of the request.

2.1.5. Rules for using the COMBRIDGE services

2.1.5.1. These rules for using the COMBRIDGE network and services apply to all COMBRIDGE clients or third parties using the COMBRIDGE network as a means of communication. COMBRIDGE will not tolerate any direct or indirect abuse by using its network even if it originates from COMBRIDGE clients (the Beneficiaries), from COMBRIDGE clients' clients or any third party using the COMBRIDGE network as a means of communication.

2.1.5.2. COMBRIDGE believes that eliminating SPAM and abuse will result in a cheaper, better and more efficient Internet for its clients.

2.1.5.3. COMBRIDGE defines as abuse or illegal use of the network:

Any commercial email (commercial communication via email) sent to an address that has not expressly requested and confirmed the desire to receive such messages. Commercial emails include, without limitation, advertisements, opinion polls, promotional offers, etc. These types of messages are called "Unsolicited Broadcast Email"/"Unsolicited Commercial Email" and will be hereinafter referred to as SPAM.

Generating unusually high traffic in order to overload the connection of a server or Internet user, or to deplete server resources by blocking the access of legitimate users. This type of abuse will be hereinafter referred to as “flood”.

2.1.5.4. Any activity aimed at accessing, obtaining and/or modifying information/resources which is/are not public. These types of activities include, without limitation, exploiting security breaches on other computers connected to the Internet, searching (scanning) for security breaches of computers connected to the Internet, using proxy services without the consent of the owner of such services.

2.1.5.5. Transmission, distribution and storage of computer viruses, programs, files or materials that violate applicable laws or are protected by copyright, trademarks, factory marks or services, or any other intellectual property rights without the necessary authorizations, without the list being exhaustive.

2.1.5.6. Transmission, distribution and storage of materials which are obscene, discriminatory, racist or which infringe export control laws.

2.1.6. COMBRIDGE rules

2.1.6.1. The COMBRIDGE network can be used by its clients to connect to other networks, and the users of the COMBRIDGE network understand that they must comply with all rules for the use of these networks. COMBRIDGE clients (Beneficiaries) understand that COMBRIDGE cannot control the information circulating through the COMBRIDGE network. Any overloading of the COMBRIDGE network will be deemed as an unauthorized use of the COMBRIDGE network and is therefore prohibited. Similarly, it is prohibited to the use of “IP multicast” without permission from COMBRIDGE.

2.1.6.2. The clients using the COMBRIDGE network are prohibited from allowing, and are not entitled to allow, the use of the COMBRIDGE network by third parties to send SPAMs and/or to misuse the COMBRIDGE service and/or network or other electronic communications networks. If mass emails are sent, the senders must keep data attesting the approval by each recipient to receive such messages before the messages are sent. If such evidence is absent, COMBRIDGE may, at its sole discretion, consider that approval has not been obtained and will consider the use of the network to be abusive. COMBRIDGE is not responsible for the content of any message, regardless if the message was sent by a COMBRIDGE client or not.

2.1.6.3. COMBRIDGE clients are responsible for ensuring that any user receiving COMBRIDGE services complies with these rules for use. COMBRIDGE clients will be liable for all direct or indirect abuses, including for abuses committed by the clients or partners of COMBRIDGE clients through the services provided by COMBRIDGE.

2.1.6.4. Any attempt to breach the network security or of abuse is prohibited. COMBRIDGE will investigate complaints about these incidents and will cooperate with legal institutions to detect the causes and perpetrators of such incidents. If COMBRIDGE receives a complaint against one of its Beneficiaries (client of a Beneficiary, partner of a Beneficiary), it will be sent to the client (Beneficiary) for resolution. If no response is received within 24 (twenty-four) hours indicating that the issue has been resolved, COMBRIDGE may block traffic to/from the IP address(es) involved in the complaint until COMBRIDGE is satisfied that the problem has been resolved and that precautions have been taken to prevent future incidents.

2.1.6.5. COMBRIDGE may block traffic to the IPs involved in the complaint, or to all of the client's IPs, until it is satisfied that security measures have been taken by the Beneficiary to prevent the incidents from reoccurring.

2.1.6.6. The traffic of clients using the COMBRIDGE network connection for activities that violate current or future legal provisions and/or the provisions of this Section or clients or users using the COMBRIDGE network for any reason may be suspended/blocked on a specific TCP/IP port or the service provided may be suspended for an indefinite period, following a 1 (one)-hour notice before or immediately, without notice, depending on the severity of the problem and/or on the damage to the network or to the COMBRIDGE services. If the service is stopped immediately, COMBRIDGE will try to contact the Beneficiary as soon as possible to inform the Beneficiary of the situation.

2.1.6.7. The clients managing an Internet domain have the obligation to set up two mailboxes: postmaster@domeniu.ro and abuse@domeniu.ro. The messages sent to these addresses should be read by persons who are able to make decisions to resolve the reported issues. Furthermore, all clients are obliged to notify to COMBRIDGE the persons who can take measures to prevent such problems from reoccurring.

2.1.6.8. In certain cases, COMBRIDGE may block the traffic to/from certain IPs that are not part of the COMBRIDGE network, if it is considered that such IPs are used to distribute SPAM, are “open relay” or are used to gain access to resources that are not public. In such cases, no client will be able to send/receive traffic from such addresses.

2.1.6.9. COMBRIDGE only communicates with its direct clients (Beneficiaries). The Beneficiary is responsible for communicating with its clients to solve any problems arisen.

2.1.6.10. The Beneficiary has the following obligations:

a. not to respond to ARP requests from the COMBRIDGE network for IP addresses other than those assigned by COMBRIDGE. For this purpose, the client is obliged not to set on interfaces directly connected to the COMBRIDGE network other IP addresses than those assigned and communicated by COMBRIDGE. This category also includes IP addresses used by the Beneficiary in the local network and which are not separated by a Layer 3 equipment (router) from the COMBRIDGE network not to activate on any interface directly connected to the COMBRIDGE network the “proxy-arp” option and it will disable it on the equipment that has it enabled by default (e.g. Cisco routers).

b. not to respond to BOOTP, DHCP and other configuration requests from the COMBRIDGE network. For this purpose, if such services are used for the Beneficiary’s local network, they must be deactivated on the interface connected directly to the COMBRIDGE network.

c. not to send to the COMBRIDGE network requests to change the routes for IP addresses other than those assigned by COMBRIDGE or belonging to the Beneficiary. For this purpose, dynamic route announcement protocols, other than those agreed with COMBRIDGE, will not be activated and used on the interface directly connected to the COMBRIDGE network, and the RIP/OSPF protocols will be deactivated.

d. not to send to the COMBRIDGE network “ICMP redirect” packets for IP addresses other than those assigned by COMBRIDGE.

e. to avoid sending to the COMBRIDGE network “broadcast” packets other than the strictly necessary ones (ARP type), and the latter must observe an algorithm to increase the query interval, reaching more than 1 (one) second if no response is received.

2.1.7. Recommendations

2.1.7.1. The Beneficiary must update COMBRIDGE about the names and contact addresses of the persons able to solve the problems described in this Section.

2.1.7.2. The Beneficiary must take all necessary measures to ensure that any user of the service provided to it by COMBRIDGE complies with these rules and the obligations laid down by the relevant legal acts.

2.1.7.3. The Beneficiary must quickly investigate any complaint received from COMBRIDGE.

2.1.7.4. When the Beneficiary sends email messages to a list of recipients, it must ensure that it has the confirmation of each recipient wishing to receive its messages.

2.1.8. Other recommendations

- The installation of an antivirus software, keeping it updated by daily checking new definitions of updates. The vast majority of antivirus software can be programmed to do this automatically.
- Ensuring that all security patches are installed, as new Windows vulnerabilities are constantly being discovered.

Viruses continue to exploit old vulnerabilities as many users do not regularly use patches. The failure to use patches will expose to risks other systems as well.

If a virus has infiltrated the computer system due to the failure to install an appropriate patch, all the persons in the personal address book become the next target.

- Using a firewall, as no Internet connection is secure without a firewall. A firewall supporting the connection must be found. Firewalls will prove useful even if the Internet connection is dial-up. In case of a broadband Internet connection, the system will become much more vulnerable to attacks.
- Securing the email. We need to make sure that we are not exposed to infections caused by the email client. Attachments are just a small part of this problem. If this service cannot be configured, it is recommended to apply patches and all the other precautions regarding attachments, as the email is the weakest link.
- Securing the browser If Internet Explorer is used, the secure zone settings can be used to ensure maximum browser security.

2.1.9. Limits of liability

COMBRIDGE bears no liability for the Beneficiary's failure to comply with the legal, contractual, present rules for use and/or the recommendations included in these rules.

2.2. The client's Internet access

The client is responsible for any incidents and changes occurred in the client's Internet access.

The Combridge officers can conduct a preliminary check only if the Smart CPE service has an enabled 3G backup.

No level of availability (SLA) is guaranteed for this service

2.3. 3G backup

Included in the **Smart CPE-A** service, the backup solution offers the following advantages:

- It prevents the operational impact and revenue losses that may occur if a location is disconnected;
- Low costs;
- Automatic switch to the backup connection when the main circuit malfunctions;

- The connectivity and data are not affected as the IP address does not change
- Unlimited traffic;
- The transfer speed for the first 8 GB is best effort (up to 225 Mbps download and up to 50 Mbps upload) and for above 8 GB it reaches up to 128 kbps download/64 kbps upload.

Combridge offers the indicated services only in the coverage area of the electronic communications provider communicated by the Manager responsible for the client, either upon Combridge's initiative or upon the client's request, at any time during the contract.

2.4. The Cloud-based management system

NMS is an enterprise-class management system based on Cloud that allows the creation of bandwidth policies and the centralized monitoring without the need to add equipment to the network.

3. Virtual Private Network (VPN)

VPN package features:

- The VPN tunnel configuration is based on the VMware virtualization;
- Scalable in relation to configuration changes and minimal effort required to reconfigure the network if access locations are added in the client's network.
- All access locations in the Client's network are integrated into the same VPN using the IPsec VPN solution for the client's Internet access and the Internet access provided by Combridge, or the MPLS VPN solution for Internet access provided by Combridge;
- It is ideal for site-to-site connections;
- Default security of data transmissions through the virtual network;
- Layer 3 IPsec VPN: the NAT (network address translation) procedure is used to map private IP addresses, thus allowing workstations with private IPs to connect to the Internet;
- It extends existing security policies, in particular those relating to Intranet access, to mobile employees;
- Routing: static or dynamic;
- The services offered on the Combridge network are secure and high quality services;
- Proactive monitoring;
- It is purchased only once and can be used for an unlimited number of locations;
- Reduction of expenses allocated to IT and predictable budget;

The **VPN Gateway Virtual Appliance** is designed to innovatively simplify the termination of VPNs for thousands of access locations in the client's network. The heart of the product is a software application for VMware compatible equipment; the soul of the product is an enterprise-class VPN concentrator capable of completing thousands of tunnels designed to remotely connect access locations in the client's network.

Branch on Demand is a cloud-based solution that simplifies the deployment, management, security, and troubleshooting for remote deployments. The central point is the Smart CPE platforms. Due to the robust operating system, the Smart CPE requires virtually no other end-user intervention than starting and connecting to the Internet. Once turned on and connected to the Internet, the equipment will automatically find its NMS, which can be located in the cloud or on the local network, will download its security policies, thus establishing the connection to the VPN. In just a few minutes, the new location will be active and visible in the VPN, and there is no need to download the configuration for each device or to train the end users on the use of the VPN.

Thanks to the unified policies for both wired and wireless communication, setting up any network for a wide range of clients becomes easy. When the equipment goes online, the NMS automatically transmits the configuration based on the device parameters. The NMS is located outside the local network, and the WAN

network malfunctions do not affect the local network or WLAN. As the NMS has a single centralized interface for configuring and managing APs and routers, the management of thousands of devices is literally the same as the management of a single device.

4. The Corporate Communication solution

It is available in 2 variants:

- ✓ **Entry Corporate Communication Solution (CCS-E) for up to 20 users.**
- ✓ **Advanced Corporate Communication Solution (CCS-A) for an unlimited number of users**

- Voice, Video, Fax, Professional Chat easily integrated with mail server, web server, security server and business applications.
- The CCS-E includes 1 (one) VPS-A
- The CCS-A includes 1 (one) VPS-S
- **The main features of the CCS (the functionalities may be optional):**

4.1. IP PBX

- It can completely replace the traditional private branch exchange (PBX).
- It provides a wide range of services, including a 100-line voice trunk, 100 telephone numbers, SIP telephone support, Soft telephone support, Fax2Mail & Mail2Fax, queue management, call forwarding (follow-me), call scheduling, call pick-up, call blocking, IVR, ENUM, call statistics, call parking and transfer, on-hold music, call conference. The generated voice traffic is not included in the monthly fee, the charging is determined according to the SIP TRUNK price list in force published on the website www.combridge.ro.
- It allows easy configuration of call groups and access classes.
- The DISA feature allows access from outside the office to all the functionalities of the telephone as if you were in the office.
- With the Fax2Mail service, any received faxes are forwarded to a predefined email address. An email is sent to a fax number via the Mail2Fax service. A PDF file can be attached to an email and sent to a fax number by simply using the mail client or via webmail.

Follow me - forwarding a call configured from the destination extension (e.g. if your extension is 200 and you work from another office, you can pick up the extension receiver where you, enter the follow me code, your extension, 200 in this case, and the extension password, and calls to the 200 extension will be forwarded to the new extension.

Call schedule - also called call distribution according to the schedule.

Call Parking - allows any user to put calls on hold.

Call Transfer - allows any user to transfer the call to another destination.

Call Forwarding - allows users to forward their incoming calls to another destination that can be both landline or a mobile telephone.

Call Pickup - allows answering a call to another telephone in the picking up group.

Conference calls - allows adding one or more participants to a call

Call blocking - allows a user to block incoming calls from a specific telephone number.

Hold-on music - plays a recorded song that fills the silence of a call that has been put on hold.

Direct Inward System Access - DISA is a feature by which a caller, after entering the code through a menu, receives a ringtone to access some or all of the PBX features, such as making a call abroad or sending a voice message.

Interactive Voice Response or IVR - allows clients to interact, in real time, with a robot by pressing the offered voice menu keys using multifrequency tones (DTMF).

ENUM - the conversion of a telephone number into an IP address.

Call statistics - the detailing of the company's calls offering an overview to the client.

Queue Management - helps organize queued calls.

4.2. Dynamic and static conference

Static and dynamic conferencing are optional features configured by the Combridge Technical Support upon the client's request.

For static conferences, preconfigured telephone numbers and PINs are assigned (e.g. telephone no. 0310800xxx, PIN: 6589 #), and only the telephone number is preconfigured, the PINs remaining at the client's choice, for dynamic conferences.

Use method:

4.2.1. Static conference - the telephone number and PIN provided by Combridge (e.g. 0310800xxx. PIN 6589 #) are used

- a. Each participant calls the preset telephone number (e.g. 0310800xxx) dialling +40 (e.g. +40310800xxx) if calling from abroad.
- b. The participant will be asked to enter the conference PIN number and will enter the preconfigured PIN followed by the # key (e.g. 6589#)
- c. The participant will be asked to say his/her name after the beep and to press the hash (#) key again afterwards
- d. The participant is asked about three other options:
 - i. Press 1 to accept name and join the conference
 - ii. Press 2 to hear names
 - iii. Press 3 to register the name again (if not heard well the first time)

Steps i, ii and iii can be repeated until the participant presses 1 and accepts the registered name and joins in the conference.

4.2.2. Dynamic conference - the telephone number provided by Combridge (0310800xxy) is used

- a. Each participant calls the number provided by the Combridge Technical Support (e.g. 0310800xxy or +40310800xxy if calling from abroad)
- b. The participant is asked to enter the conference ID followed by the # key

The first participant or the organizer of the conference can set the conference ID; it is important to send the telephone number and the ID of the conference to all participants. If one of the participants enters a wrong ID, he/she actually initiates a new conference.

- c. The participant will be asked to enter the conference PIN number and will enter the PIN followed by the # key.

The first participant or the organizer of the conference will set the conference PIN followed by the # key (it does not have to be a fixed PIN, it can consist of 3 or 4 digits, at choice, followed by the # key). The other participants will enter the PIN created by the first participant in the conference, a PIN sent in advance to all participants.

- d. The participant will be asked to say his/her name after the beep and to press the hash (#) key again afterwards
- e. The participant is asked about three other options:
 - i. Press 1 to accept name and join the conference
 - ii. Press 2 to hear names
 - iii. Press 3 to register the name again (if not heard well the first time)

Steps i, ii and iii can be repeated until the participant presses 1 and accepts the registered name and joins in the conference.

The number set for the dynamic conference can host simultaneously as many conferences as desired; it is important to set a separate PIN for each conference, that conference participants do not join an ongoing conference; more complex PINs are recommended for very important conferences.

4.3. Hosting

Virtual hosting is a simple, flexible, high-quality solution that offers the possibility to host, within the space on the disk the CCS is configured on, a mail server, an FTP server and an unlimited number of domains and websites without allocating dedicated resources responsible for maintaining the hosting solution.

The email and groupware solution allows clients to exchange emails, manage their calendar and address book. This service includes antivirus, anti-spam filtering, updates, browser access, email client and calendar integration. You can access your emails, contacts and also consult, manage and distribute your calendar and activities on a secure and fully integrated platform.

4.4. Security

The security platform is a scalable method to manage the security risks that company applications may face using an IP packet filtering firewall, explicit proxy, content filtering, and reverse proxy.

The **proxy mode** can be used for any important service such as STMP, HTTP/HTTPS, FTP, Skype and Messenger.

The **content filtering** can be applied for filtering websites based on the domain, such as ads, games, adult content, etc.

4.5. Domain Server

It allows administrators to dynamically segment, at no additional costs, their Windows system into isolated and secure networks based on security policies using the protocol **LDAP** while integrating with **Active Directory, Radius Server**, the **DHCP** protocol, the **DNS** protocol, **printer servers and databases**.

4.6. DDoS Protection

A DoS (Denial of Service) or DDoS (Distributed Denial of Service) cyberattack is a fraudulent attempt to render a server/service unavailable or to block it. Although the means and objectives of carrying out this attack are very diverse, such attack is in general the effect of the intense efforts of one or more people to prevent a server/service from operating efficiently, for a temporary or unlimited period.

By using sensors to detect attack occurred at the network's boundary, every IP receiving Internet traffic through the Combridge network can be protected against any type of DDoS attack.

When suspicious traffic is detected, the traffic to that IP is redirected to a secure Cloud, mitigating the impact to the client and maintaining a constant latency. The process of detection, filtering and diversion of the

default route is fully automatic and its effectiveness is emphasized by the countermeasures taken in real time and which are totally transparent for the end client.

The resources to be protected are decided based on special route map and on a BGP announcement. The route map must be updated with the ASNs/AS-sets to which the prefixes to be protected belong. Moreover, protected prefixes must be notified via BGP to Combridge.

Only real traffic is delivered to the client's equipment.

5. VPS - Virtual Private Server

- The VPS servers are configured on a physical server installed in Bucharest in a secure Tier 3 colocation centre, with backups performed automatically and disaster recovery capabilities.
- Available operating systems: Centos, UBUNTU, Free BSD, Debian, Windows
- Optimal performance, security and maximum availability
- Available in the client's VPN
- Additional Cloud-based processing power
- 3 products:
 - Easy VPS (**VPS-E**)
 - Advanced VPS (**VPS-A**)
 - Star VPS (**VPS-S**)
- Each VPS includes 1 (one) public IPv4 or IPv6 address
- 99.9% SLA
- Characteristics:

	Easy	Advanced	Star
Storage	Yes	Yes	Yes
Storage type	HDD	SSD	SSD
Storage space	10 GB	30 GB	100 GB
Guaranteed RAM	1 GB	4 GB	16 GB
Maximum RAM	2 GB	8 GB	20 GB
CPU	1c @ 2 GHz	1c @ 2 GHz	1c @ 2 GHz
vCPUs	1	1	2
Traffic	Unlimited	Unlimited	Unlimited
Network port	1 Gbit	1 Gbit	1 Gbit

A minimum of 50 GB of storage must be allocated for Windows instances.

- The resources on the 3 VPSs can be supplemented, on request, with a multiple of 2 GB of RAM and a multiple of 100 GB of storage space.

5.1. VPS service use policy

5.1.1. The Beneficiary is not permitted to use the Provider's network and services to transmit, distribute or store material (a) that violates any applicable law or regulation, including the law of other countries from where the access to VPS is possible (b) in a manner infringing copyright, trademarks, trade secrets or other intellectual property rights or the right to privacy, advertising or other personal rights of other parties, (c) if it is dishonest, obscene, defamatory, slanderous, threatening, abusive or contains a virus, worm, Trojan horse, or any other component likely to cause damage, (d) that contains fraudulent offers of goods or services or other promotional materials containing false statements, claims or representations, likely to deceive or mislead, or (e) in general, in a manner that may incur the criminal or civil liability of the Provider or any of its employees.

5.1.2. The Provider assumes no liability for any material created or accessible on or through the Provider's networks and services which is not sent by the Provider or at the Provider's request. The

Provider does not monitor or exercise any editorial control over any such material, but reserves the right to do so to the extent permitted by the applicable law.

5.1.3. The Provider is not responsible for the content of any web site other than those of the Provider.

5.1.4. The users - clients are not allowed to send unsolicited email messages, including, without limitation, ad packages.

5.1.5. (1) The Beneficiary undertakes not to infringe or attempt to infringe the security of the Service Provider's Network, including, without limitation: (a) accessing data that is not intended for the client or entering a server or account the Beneficiary is not allowed to access, (b) attempting to scan or test the vulnerability of a system or network or to breach its security or authentication measures without proper authorization, (c) attempt to interfere with, interrupt or render unusable the service of another user, host or network, including, without limitation, by overloading, "flooding", "mailbombing" or spamming, i.e. sending large amounts of email or other information to an individual email address or to another user of the service, (d) counterfeiting any TCP/IP header or any part of the information contained therein when sending by email or to a Usenet group or initiating any action in order to obtain services to which the Beneficiary is not entitled.

(2) In order to protect the Provider's network, the Provider's resources, as well as the other clients of the Provider, in case of Denial-of-Service attacks targeting Internet addresses, the Provider reserves the right to take the necessary measures to minimize the effects of such incidents. The measures may include, without limitation, temporarily blocking the addresses or classes of addresses under attack throughout the Provider's network.

(3) The Provider reserves the right to delete any information entered by the Beneficiary in its system and which may cause the failure or improper operation of the Provider's network. (4) The Beneficiary is responsible for the protection of its IT system and for the integrity of the data entered in the Provider's system.

5.1.6. The use of the following scripts on the Provider's servers is not permitted:

- UltimateBBS
- Any script or platform that allows Content Sharing (torrent, dc, etc.)
- IkonBoard
- All YABB forum versions
- Proxy scripts
- IRC scripts (ircbots, psybnc, etc.)
- Anonymizer
- Phishing
- Chat rooms, not including standard dashboard scripts
- PhpShell and similar scripts for executing commands
- FormMail
- Other scripts and applications that have vulnerabilities or dangerous behaviour.
- Installation of game instances (Counter Strike, Half-Life, Minecraft, etc.)
- Installing and using Shoutcast or any similar audiostreaming software
- Installing and using Wowza or any similar videostreaming software
- Installing and running public mirrors
- Hacking, warez sites or sites promoting activities that are illegal or barred by law
- Installing and running web-spiders or crawlers
- Installing/running scripts that generate DDOS attacks
- Scripts that test and/or exploit vulnerabilities in any operating systems, equipment, platforms, or websites.

5.1.7. The Provider will implement any requests and decisions of the competent bodies and institutions, including criminal bodies and courts, regarding the refusal of the client's access to the service, the provision of any information about the client (including identification data, payment method, invoices). In such cases, there is no obligation to inform the client in advance or to perform any other formality, and the Provider cannot be held responsible for the breach of confidentiality.

5.1.8. The Beneficiary represents to have understood and to accept that it is solely responsible, without limitation, for violating any of the above prohibitions, and that, in such cases, the Provider has the right to change, block, suspend, terminate the provision of the service and delete the content of the Server, without any prior formality, and the Beneficiary will immediately indemnify the Provider for any and all damages caused by the violation of these provisions.

5.1.9. The Beneficiary represents, accepts and undertakes to comply with any notices, warnings sent by the Provider or published on the website during the use of the Services.

5.1.10. The Beneficiary represents to have understood and to accept that the service provided is the exclusive property of the Provider and that the intellectual and industrial property rights for any software, design, program or any other content related to the service belong exclusively to the Provider. In case of finding any violation of these rights of the Provider, committed by the client, the Provider reserves the right to immediately cease the provision of the Service, to delete the content of the Server while initiating any legal proceedings it deems necessary.

6. Managed LAN

Complete solution that includes the provision of the IT infrastructure, its management and monitoring as well as the development of customized disaster recovery solutions allowing the client to fully control its applications and data.

Characteristics:

- A new infrastructure
- Cloud-based management
- Unified policies for both wired and wireless communication
- Enterprise-class security
- PoE
- Zero-touch deployment
- QoS
- 24/7/365 technical support
- Proactive monitoring
- Equipment change on the Next Business Day

Equipment:

Small Branch 8 port switch (MLAN-8P)

Ideal for Retail/Small Branch, Conference Rooms (Fanless, 1GE Uplinks, PoE)
 PoE ports: 8PoE/PoE+GE
 PoE maximum power: 124 W
 Uplink capacity: 2 x 1GE Combo (SFP or Copper)
 Switching capacity: 20 Gbps

Enterprise Class 48 port switch (MLAN-48P)

Enterprise Class Premium
 Ideal for: deployment of small and medium-sized campuses (High power budget, 10GE Uplinks, for clients ready for HMNG) E.g. K-12, Enterprises, Universities
 PoE ports: 48 PoE/PoE + GE
 PoE maximum power: 740W
 Uplink capacity: 4 x 10GE SFP+

Enterprise Class 24 port switch (MLAN-24P)

Enterprise Class Premium
 Ideal for: deployment of small and medium-sized campuses (High power budget, 10GE Uplinks, for clients ready for HMNG) E.g. K-12, Enterprises, Universities
 PoE ports: 48 PoE/PoE + GE
 PoE maximum power: 370W
 Uplink capacity: 4 x 10GE SFP+
 Switching capacity: 128Gbps

*Ordering codes: **MLAN-8P-SEL-1YR/3YR, MLAN-24P-E-SEL-1YR/3YR, MLAN-24P-A-SEL-1YR/3YR, MLAN-48P-SEL-1YR/3YR, MLAN-8P-CON-1YR/3YR, MLAN-24P-E-CON-1YR/3YR, MLAN-24P-A-CON-1YR/3YR, MLAN-48P-CON-1YR/3YR***

7. Managed WLAN

It allows the use of a wireless network to create a more flexible work environment, in order to increase business flexibility.

Characteristics:

- Cloud-based management
- Unified policies for both wired and wireless communication
- Enterprise-class security
- PoE
- Zero-touch deployment
- Interoperability with various brands on the market
- 24/7/365 technical support
- Proactive monitoring
- Equipment change on the Next Business Day

Excellent flexibility given by 10 different types of APs:

1. **MWL-122** - Basic Dual Band Access Point - 2x300 Mbps Internal Antenna (Indoor; Dual Radio 802.11n or 11n/ac; TPM Security Chip & PPSK; 1xGEth interface; 1xPOE; USB; 0°C - 40°C)
2. **MWL-130** - High Density Dual Band Access Point - 300+867 Mbps Internal Antenna (Indoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; 1xGEth interface; 1xPOE; no USB; 0°C - 40°C)

3. **MWL-230** - High Density Dual Band Access Point - 450+1.3 Gbps Internal Antenna (Indoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; 2xGEth interface with Link Aggregation; 1xPOE; USB; 0°C - 40°C)
4. **MWL-245** - High Density Dual Band Access Point - 450+1.3 Gbps Ext. Antenna (Indoor; Dual Radio 802.11ac/n Wave 2; TPM Security Chip & PPSK; 2xGEth interface; 1xPOE; USB+BLE; 0°C - 50°C)
5. **MWL-250** - High Density Dual Band Access Point - 1.3+1.3 Gbps Int. Antenna (Indoor; Dual Radio w/ a Software Selectable Radio 802.11ac Wave 2; TPM Security Chip & PPSK; 2xGEth interface with Link Aggregation; 1xPOE; USB+BLE; 0°C - 40°C)
6. **MWL-550** - Extreme Performance Dual Band Access Point - 1.7 +1.7 Gbps Int. Antenna (Indoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; ; 2xGEth interface with Link Aggregation; 2xPOE; USB+BLE; 0°C - 40°C)
7. **MWL-1130** - Outdoor Access Point IP67 - 300 + 867 Mbps Ext Antenna (Outdoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; 1xGEth interface; 1xPOE; no USB; - 40°C - 55°C)





Ordering codes: **MWL-122-CON-1YR, MWL-130-CON-1YR/3YR, MWL-230-CON-1YR/3YR, MWL-245-CON-1YR/3YR, MWL-250-CON-1YR/3YR, MWL-550-CON-1YR/3YR, MWL-1130-CON-1YR/3YR, MWL-122-SEL-1YR, MWL-130-SEL-1YR/3YR, MWL-230-SEL-1YR/3YR, MWL-245-SEL-1YR/3YR, MWL-250-SEL-1YR/3YR, MWL-550-SEL-1YR/3YR, MWL-1130-SEL-1YR/3YR**

7.1. Self-Registration Manual

After connecting to the wireless registration network, a web page will be automatically opened to enter the connection details received from Combridge. If there are several locations, each location will have its own name of the registration network, e.g.: client name-Guest-Ploiești-Registration, client name-Guest-Constanța-Registration, etc. All networks will add users to the same database and the created users are valid for 7 days and will be able to connect to any location.

Fill in the fields of the web page, as in the example below, and click on Register:

First Name: Test;
 Last Name: Testing;
 Email: test@yahoo.com (it will not send an email with login details);
 Telephone: 1234567 (it will not send an sms);
 Visiting: mircea.marin@Combridge.ro (it will not send a confirmation email);
 Comment: (not mandatory).

<p>Secure Internet Portal</p> <p>New users should fill out the form below to request a private preshared Key for accessing the secure wireless network.</p> <p>First Name*</p> <p>Last Name*</p> <p>Email*</p> <p>Phone</p> <p>Visiting*</p> <p>Comment</p> <p>It may take a moment for registration to complete (* required).</p> <p>Register </p> <p>Powered by  Aerohive NETWORKS</p>	<p>Secure Internet Portal</p> <p>New users should fill out the form below to request a private preshared Key for accessing the secure wireless network.</p> <p>Test</p> <p>Testing</p> <p>test@yahoo.com</p> <p>+40784277418</p> <p>mircea.marin@combridge.ro</p> <p>no comment</p> <p>It may take a moment for registration to complete (* required).</p> <p>Register </p> <p>Powered by  Aerohive NETWORKS</p>
--	--

Secure Internet Portal

Thank you for registering.

Please use the following Private Pre-Shared Key to access the secure SSID: **YaN208CU**

Login page

Powered by  **Aerohive**

The login password and the network to connect to for Internet access will be displayed on the screen.

NOTE: The password must be copied and saved to a file as it is not possible to save it automatically.

Connect to the guest Internet network using the password provided by the Secure Internet portal upon registration, according to the steps mentioned in this chapter, and click on Next.

8. Voice Headsets

8.1. Basic (VHB)

VHB1610 - GXP1610: 1 line; 3-way conference; security: SIP/TLS, SRTP, AES-256, 802.1x.

VHB303 - SPA303-G2: 3 lines; 3-way conference; security: SIP/TLS.

VHB19P - T19P: 1 line; 3-way conference; security: SRTP, TLS.

8.2. Medium (VHM)

VHM1628 - GXP1628: 2 lines; 3-way conference; Gigabit Port; Security: SIP/TLS, SRTP, AES-256, 802.1x.

VHM514 - SPA514G: 4 lines; 3-way conference; Gigabit Port; Security: RFC 1321; AES-256; SIP/TLS; SRTP

VHM23G - T23G: 3 lines; 3-way conference; Gigabit Port; Security: SRTP, TLS

8.3. High End (VHHE)

VHHE2170 - GXP2170: 12 lines; 5-way conference; Gigabit Port; Bluetooth; Security: SIP/TLS; SRTP

VHHE8861 - 8861: up to 10 lines; 3-way conference; Gigabit Port; Bluetooth; Security: AES; SIP/TLS; SRTP

VHHE29G - T29G: 12 lines; 3-way conference; Gigabit Port; Bluetooth; Security: AES-256; SIP/TLS; SRTP

8.4. Extension Set (VHEX)

VHEX2000 - GXP2200EXT: compatible with GXP2170

VHEX8800 - CP-BEKEM: compatible with Cisco 8861

VHEX20 - EXP20: compatible with Yealink T29G

*Ordering codes: **VHB1610, VHB303, VHB19P, VHM1628, VHM514, VHM23G, VHHE2170, VHHE8861, VHHE29G, VHEX2000, VHEX8800, VHEX20.***

9. Linkyfi

Linkyfi is a public hotspot platform combining visitor access management with WiFi and WiFi marketing. It is an efficient service that improves the WiFi experience of end users.

Linkyfi is a simple marketing tool that uses the mechanism of conditional access to the Internet to collect data about its users. To browse the Internet for free, the client, encouraged by the possibility of benefiting from a discount or other attractive offers, connects to the Linkyfi platform. When connected, the client can choose the method of accessing the free WiFi - by entering the telephone number or email address, connecting through social media accounts or by completing a short questionnaire. An in-depth analysis of the client information allows the business owner to create and send customised advertising campaigns to clients at the email address or telephone number provided. In addition, the client can be offered the possibility to use the virtual menu, virtual points/virtual stamps or to navigate to selected places. The Linkify platform offers a wide range of possibilities, being suitable for various facilities, such as hotels, restaurants, airports, railway stations, malls, cinemas or even mass events.

Features and benefits:

- Market research, reports, statistics that provide reliable information about each client, so that the business owner can properly adjust the offers according to the client's needs.
- Promotional campaigns targeting each client, in order to establish a direct contact with the client.
- Virtual stamps are the loyalty cards of the next generation, their purpose being to increase the attractiveness of the brand and to have an improved relationship with the client.
- Customised advertising campaigns that are easy to prepare and adapt to the needs of each client and that ensure an increased efficiency of the advertising campaigns.
- Mobile advertising offers the company owner the opportunity to send advertising campaigns directly to the client's mobile, ensuring a brand awareness increase among clients
- The interior localisation collects information about the mode and direction of movement of each client, optimising the sales and advertising space, increasing staff efficiency.
- The license is purchased once a year and is available in both 1-year and 3-year versions.
- The product is available in 3 variants:
 - **Linkyfi Basic** (LBA/C/1 and LBA/C/3)
 - **Linkyfi Plus** (LPL/C/1 and LPL/C/3)
 - **Linkyfi Pro** (LPR/C/1 and LPL/C/3)

Characteristics

Applications	Features	Basic	Plus	Pro
Dashboard	Last 24 hours - New clients/Return clients	+	+	+
	Average duration			
	Visits			
	Connection history and histogram			
	Logged in clients			
	Login type			
Captive portal	CP editor	+	+	+
Marketing	Questionnaires	-	+	+
	Wizard interface			
	Report			
	Marketing campaigns			
	Birthday campaigns			
	Advertisement			
	Loyalty			
	Results			
Geographic marketing	Interior localisation	-	-	+
	Editor			
	Heatmaps			
	Movement method			
	KPIs for defined groups			
	Event-based marketing			
	Captive portals			
	SMS			
	email			
	Facebook posts			
Statistics	Logged in clients	-	+	+
	Global traffic			
	Demography			
	Connection history and histogram			
	Operating systems			
	Devices			
	Personal information			
Multi-tenancy	Aggregate data by level within the organization	-	+	+
	Permissions per unit			
	Permissions per user			
Linkyfi wallet		-	+	+

- No product content + Product content

10. Network management

- Access network management - MWL-CMBW-ANM - HiveManager NG Perpetual license for one (1) AP device or switch. The license is purchased annually.
- Routing network management - MWL-CMBW-RNM - HiveManager Classic Perpetual license for one (1) AP device, router or switch. The license is purchased annually.

10.1. MWL-CMBW-ANM

The Access Network Management virtual application is an on-premises version, usually deployed in the client's private network, in the client's data centre. It has the same enterprise-level network management functionality as the public cloud version, NMS, mentioned in the chapters above. The difference lies in the installation and management characteristics specific to the deployments in the client's location. The key benefits include:

- Dashboard: intuitive visual dashboard with context filters for a comprehensive overview of the network devices, state cards with KPIs in the network, application and data usage, and user activity.
- Application visibility and control: Visibility and control of the use of applications in the network for professional and recreational applications.
- Simplified deployment: Workflows for creating and deploying network policies, with advanced optional configuration.
- Monitoring: real-time viewing of devices, clients, alarms and events. Ability to collect device information directly from the monitoring interface.
- Troubleshooting: Optimized Help-Desk interface to query a client's history and its real-time problems with concrete data to reduce escalation and provide a better end-user experience.
- Unified network management: Management using a single management console of both wireless and wired devices.
- Open APIs: access to APIs for monitoring, identity and configuration services.
- Guest access: Boarding and managing personal devices for visitors and employees.

10.2. MWL-CMBW-RNM

The Routing Network Management system allows the creation of simple policies, firmware updates, configuration updates and centralized monitoring from a single console. This system combines APs, routers and switches with a suite of cooperative control protocols and features to provide unified access, both wireless and wired, ensuring a consistent policy, permissions and security according to the identity and the type of the device, regardless of the user location. The Routing Network Management provides a centralized management console for the entire network, allowing a global policy, configuration and monitoring with full visibility of thousands of APs, routers and switches. The Routing Network Management reduces operating costs by accelerating the deployment, configuration and monitoring of the entire network.

The key benefits include:

- Customisable dashboard with application visibility and control based on the user identity
- Unified policies, configuration and reporting separated by wireless, switching, routing, VPN, IP address management, and security policies.
- The Express mode designed for deploying Wi-Fi networks
- The Enterprise Advanced mode intended for large organizations with sophisticated policy requirements
- Integrated scheduler, Package Capture, client tracking tools to facilitate remote deployment and troubleshooting
- Spectrum analysis to detect and identify sources of non-WiFi interference in the 2.4 GHz and 5 GHz bands;
- Client device and operating system reporting system

- Client device and operating system reporting by usage, SSID trends, and client distribution across devices.
- Web application with a robust interface available on Windows, Linux, or MAC OS X with advanced features such as zero-configuration deployment, integrated IP address management providing unified management, monitoring, and remote visibility for all your devices.

11. SLA and Fault Reporting Procedure

11.1. SLA - Service Level Agreement

11.1.1. SLA calculation method

$$\text{Availability/month} = \frac{((\text{Total monthly uptime})^* - (\text{Total Downtime}))}{(\text{Total monthly uptime})} \times 100$$

Total monthly uptime = total number of minutes per month during which the service must be operational

Total downtime = number of minutes during which the service is completely non-operational

*If the duration of the service is less than one month, the time fraction will be taken into account;

When determining the downtime, the periods of Service downtime due to causes not attributable to the Provider will not be taken into account, including any malfunctions of the operational systems and services owned by the client or provided by third parties. By way of example, the lack of access to the client's Internet service provided by a third party, malfunctions and interruptions in the provision of other services by third parties - electricity, etc.

11.1.2. The CPE-A, IACC, VPN, CCS-E, CCS-A service

Guaranteed uptime: 99.5%, otherwise the client may request penalties according to the grid below; however, the total penalties cannot exceed 100% of the monthly service charge.

Between 99.5% and 98.0%	5% of the monthly service charge
Between 98.0% and 97.0%	10% of the monthly service charge
Between 97.0% and 96.0%	15% of the monthly service charge
Less than 96%	20% of the monthly service charge

11.1.3. The VPS-E, VPS-A, VPS-S service

Guaranteed uptime: 99.9%, otherwise the client may request penalties according to the grid below; however, the total penalties cannot exceed 100% of the monthly service charge.

Between 99.9% and 98.0%	5% of the monthly service charge
Between 98.0% and 97.0%	10% of the monthly service charge
Between 97.0% and 96.0%	15% of the monthly service charge
Less than 96%	20% of the monthly service charge

11.2. Fault Reporting Procedure

The fault reports issued by the Beneficiary must include the following:

- the name and contact details of the client, including the telephone number of the person reporting the fault
- Address or location where the fault occurred
- Name and telephone number of the person in charge of the indicated location
- Fault type

The person who reported the fault will receive a trouble ticket (TT) number for further reference.

- 1) The service unavailability must be confirmed or denied after the test procedures. The confirmation/denial must be made by email or fax filled in with the name of the person who performed the tests.
- 2) In case of technical troubles, the client must inform the Provider about the complaint, must cooperate to locate and identify the service interruption and to restore it.

Comment:

All confirmation forms must contain a start date and an end date of the fault, the location of the fault, the cause of the fault and the solution for restoring the service.

Incidents are reported by telephone or email to the following contact points:

COMBRIDGE Non-Stop Helpdesk:

- a. by telephone, to the numbers: +40.31.080.0000 / +40.751.291.695
- b. by email, to the address: support@combridge.ro daily, 24/7 h

The information required to open the ticket (incident note):

- Contact person;
- Detailed description of the fault;
- Telephone number;
- Fault start date/time;
- Service details (the technical details received during the commissioning of the service)

The ticket is confirmed via email.

After verifying the claimed issues, the Combridge support team will send a response to the client, within 1 (one) hour of receiving the trouble ticket. The response will consist of information about the nature of the fault and the repair time.

The repair time will be determined according to the nature of the fault, and it may take up to 4 (four) hours.

If the client is not satisfied with the manner in which the incident is solved, the client can request via support@combridge.ro to be sent additional contact details of the responsible persons within the company, so that it can submit its application to these persons.

This copy is the original of Annex No. 1 Technical Specifications for Combridge Products and Services and it is signed in witness thereof by Levente-Andras Ccenteri - Executive Manager.

Levente-Andras Csenteri - Executive Manager

**THE NATIONAL UNION OF BAR ASSOCIATIONS IN ROMANIA
THE BUCHAREST BAR ASSOCIATION**

NOTARIAL CERTIFICATE NO. 14

YEAR 2018, MONTH JUNE, DAY 27

Before me, Cinca Cristina, lawyer with the Individual Law Firm Cinca Cristina, member of the Bucharest Bar Association, came:

Csenteri Andras-Levente, Romanian citizen, domiciled in Sfântu Gheorghe, Str. Vânătorilor, Nr. 32, Jud. Covasna, holder of the ID Card series KV no. 391205, issued by SPCLEP Sfântu Gheorghe on 20.03.2017, personal identification number 1680420264441

Who, after reading the deed, represented to agree with all its provisions, for which reason he consented and signed all its copies.

As per Article 3 (1) (c) of Law 51/1995, the date, the identity of the party and the content of this deed are certified.

Lawyer Cinca Cristina